

Federal Bridge Certification Authority EMA Challenge 2000

- Background
- Overview
- Test structure
- Participants
- Results
- Conclusions and lessons learned
- Path forward

Background

- FBCA is non-hierarchical, peer-to-peer “hub”
- Supports interagency PKI technical interoperability
- Policy interoperability framework established by FPKI Policy Authority
- Goal: accommodate Federal agency use of any PKI COTS product

Overview

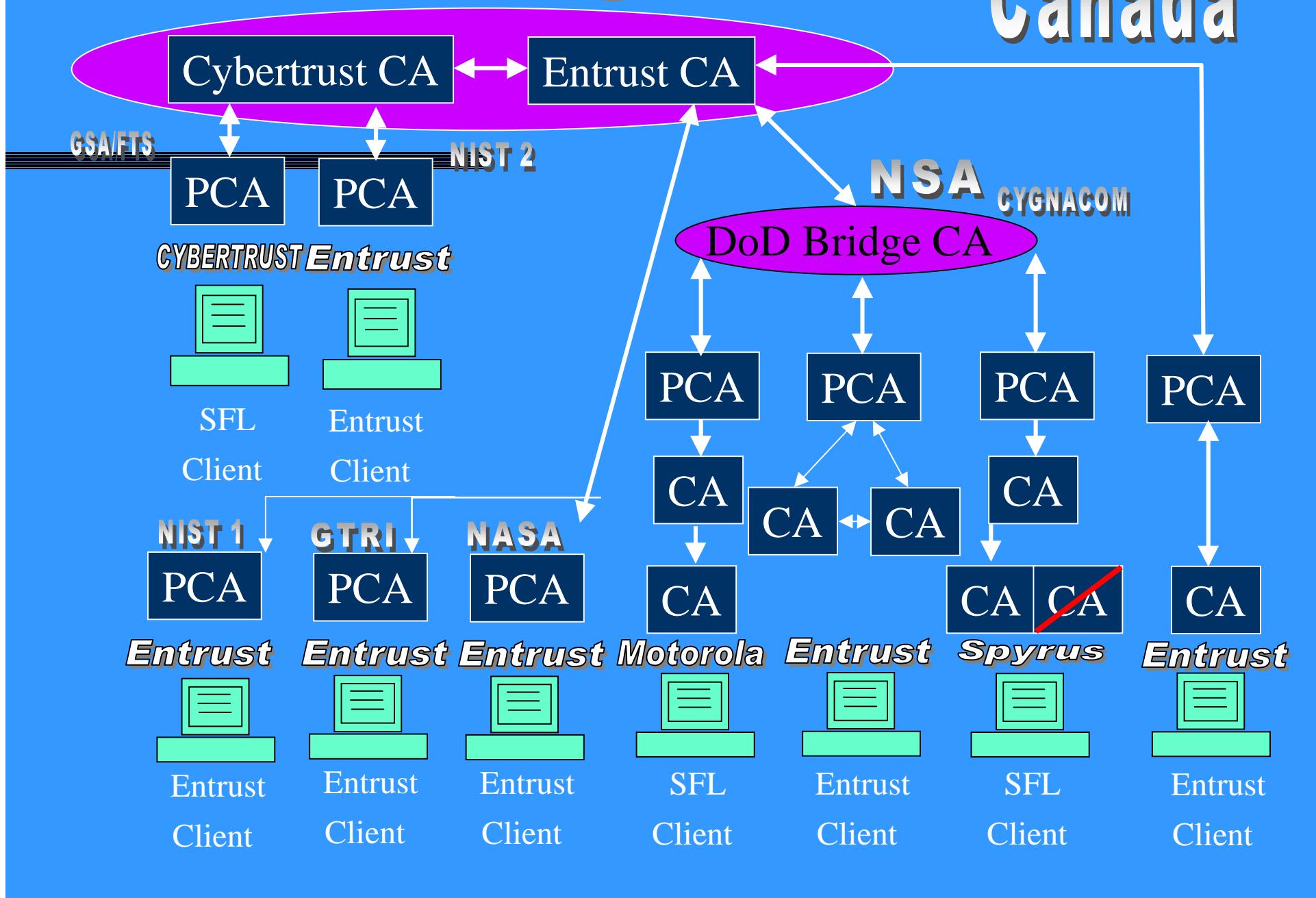
- Prototype FBCA operational 2/8/00
 - GSA auspices; hosted by Mitretek Systems
 - Entrust and Cybertrust CAs
 - PeerLogic i500 directory
 - Supports EMA Challenge and testing
- Production FBCA operational late 2000
 - Additional CA products within membrane
 - Mesh arrangement within membrane

Test Structure

- Six disparate PKI domains cross-certified with FBCA
 - Five different CA products
 - Five different X.500 directory products
- Interoperability demonstrated via exchange of signed S/MIME messages
- X.500 directory framework - chaining between directories, client access via LDAP

Federal Bridge CA

Canada



Client Details

- Eudora engineered with:
 - Entrust toolkit ("out of the box")
 - CygnaCom libraries
 - JGVanDyke libraries
- Spyrus LYNKS cryptocards for CygnaCom/JGVanDyke enabled client
- Private key on hard disk for Entrust enabled client

Participants

- Government of Canada
 - NSA/DOD
 - NIST
 - NASA
 - GSA
 - Georgia Tech Research Institute
-
- CA products: Entrust; Cybertrust; CygnaCom; Spryus; Motorola
 - Directories: PeerLogic; ICL; Nexor; CDS; Chromatix
 - Integrators: Mitretek; JGVanDyke; GNS; Booz Allen; CygnaCom; A&N Associates

Results

Conclusions and Lessons Learned

- FBCA concept works
- Client ability to develop and process trust path straightforward to implement
- Directory interoperability is critical to PKI interoperability
- Directory entries must line up with CAs
- Lots of details, lots of devils

Path Forward

- Complete testing (get all domains to interoperate fully) and prepare report
- Proceed to develop production FBCA
- Stand up FPKI Policy Authority under Federal CIO Council
- Test encryption and policy mapping
- Get trust path creation and processing capability into applications